**Pestov Maxim Alexandrovich**
Student
Ural Federal University
Russia, Ekaterinburg
**Academic supervisor: Kovaleva Alexandra Georgievna**

## INFORMATION SECURITY FROM SPYWARE

***Abstract.*** *In the modern world, much is decided by the means of information, not only located in the computers of various companies, but also among ordinary users. Passwords, e-mail addresses, personal information are the most important issues of information security. For many companies such data are of great interest. The collection of this type of information is simplified by the appearance of a large number of spyware programs, including malicious ones, which begin to monitor our every action. This paper describes main methods of protecting information from spyware.*

***Keywords:*** *Spyware, computer security, information security, data leakage, unauthorized access.*

**Пестов Максим Александрович**
Студент
Уральский федеральный университет имени первого
Президента России Б.Н. Ельцина
Россия, г. Екатеринбург
**Научный руководитель: Ковалёва Александра Георгиевна**

## ЗАЩИТА ИНФОРМАЦИИ ОТ ШПИОНСКИХ ПРОГРАММ

***Аннотация.*** *В современном мире многое решает информация, и не только находящаяся на компьютерах различных компаний, но и у простых*

*пользователей. Это могут быть пароли, адреса электронной почты, личная информация и т.д. Для многих фирм такие данные представляют большой интерес. Упрощает сбор этих сведений появление большого количества шпионских программ, в том числе и вредоносных, которые начинают следить за каждым нашим действием. В этой статье рассмотрены основные методы защиты информации от программ-шпионов.*

***Ключевые слова:*** *Шпионские программы, компьютерная безопасность, информационная безопасность, утечка данных, несанкционированный доступ*

## INTRODUCTION

According to the researchers, the task of ensuring information security should be solved systematically. This means that various security measures (hardware, software, physical, organizational) should be applied simultaneously and under centralized control. At the same time, the system components should «know» about each other's existence, interact and provide protection against both external and internal threats. Today, there is a large arsenal of methods to protect information from spyware [2].

## WHAT IS SPYWARE

Spyware is one of the most common types of unwanted software designed to collect unauthorized data from a user's device. Their popularity is due to their simplicity and demand. Many spyware programs can be legal and even distributed in official app stores. They are used, for example, to collect information about the device's location, sites visited, computer configuration, software used, keyboard input, and so on. As a rule, spyware does not have any malicious functions expressed for the victim's device, but it can cause leakage of confidential data and violation of privacy.

The destructive potential of such programs is quite high. On a modern computer with the Windows operating system, any program that an administrator or a user with the rights installed has access to all files in the system. This allows transferring data and access all information without permission [2].

Unlike the creators of viruses and Trojan horses, the authors of spyware programs need user confirmation to install the product on the victim's computer. Of course, users' attention is diverted from this procedure in various ways. Some programs use Windows with certificates and licenses, where you need to confirm reading by clicking «OK». Since these legal documents are rarely read by users and contain a number of complex wording, this is the easiest way to install a «spy» on a computer along with any popular freely distributed program. Legally, manufacturers, having received consent to install a program on a computer and transfer information from it, may declare that the product is not a «spy» and is installed after receiving permission from the user.

Immediately after installation, these programs may transmit any information from the moment the computer is connected to the Internet. Data transfer occurs in the background and is very difficult to track. The most common security programs are designed for external attacks and do not track information flows from a protected computer [5].

## HOW TO DETECT SPYWARE

Even if the spyware is well hidden, you may see traces of its presence. For example, a slow computer may be a sign of infection. You should pay attention to the following «symptoms»:

- the device is running slowly and the response time is extended;
- advertising messages and pop-UPS appear unexpectedly;
- there are new toolbars, search engines, and home pages that were not installed;
- the battery is draining too fast;
- problems occur when logging in to secure sites (if you managed to log in on the second attempt, it is possible that the first attempt was on a fake version of the site and your password was passed to hackers);
- too much traffic is being consumed. It means that the spyware is searching for your data and sending it to others;

- antivirus and other security software don’t work [1].

## USER IDENTIFICATION AND AUTHENTICATION

These procedures are performed, if technical tools that can be used to determine the identity and authenticity of the user's credentials in two stages are used. It is necessary to note that identification does not necessarily establish identity. It is possible to accept any other identifier set by the security service [5].

This is followed by authentication – the user enters a password or confirms access to the system using biometric indicators (retina, fingerprint, etc.). In addition, authentication is used by USB tokens or smart cards. However, this option is less reliable, since there is always a possibility of their loss and use by third parties [3].

There are some recommendations for the effective use of authentication systems. First, strong and unique passwords for all your accounts should be used. To avoid remembering them all, password managers may be applied. These are special programs designed to securely store and generate your passwords. In this case, it is necessary to remember only one password from this program. This is much more convenient. Two-factor authentication should be enabled – one-time codes in SMS or in the app. Otherwise, anyone who finds out your credentials may easily access an account without any confirmation.

## DATA ENCRYPTION

Data encryption is a great way to keep valuable information secure when transferring data over the Internet, backing it up on cloud servers, or storing it on a disk as usual. Data encryption prevents confidential information from being viewed by anyone. Disk encryption uses special software or hardware that encrypts every bit of storage. It is necessary only to enter a password to access the data. Currently, there are two popular software programs that allow encrypting a disk in Windows operating systems: using the built-in BitLocker encryption tool, or using a third-party VeraCrypt program [1].

## FIREWALLS

Firewalls are software or hardware and software products designed to block unwanted traffic. The firewall allows or denies access based on the parameters set by the administrator. The following parameters and their combinations can also be used:

- IP addresses: a firewall may be used to grant or deny receiving packets from a specific address, or set a list of prohibited and allowed IP addresses.
- Domain name allows setting a ban on skipping traffic from certain websites.
- Ports: setting the list of forbidden and allowed ports allows regulating access to certain services and applications. For example, if the port 80 is blocked, the access of websites is prevented.
- Protocols: The firewall can be configured to block traffic from certain protocols.

A firewall configured solely on the basis of access permissions warns of any attempt by an application to transmit data over the network and allows blocking this operation, thus drawing the administrator's attention to applications that may turn out to be spyware [4].

## CONCLUSION

According to the results of the research, we can say that stealing of confidential data through spyware is currently a very popular method of obtaining information by unscrupulous competitors. This method is the least risky and does not require additional hardware, except for the malware itself. The attacker only needs to show social engineering skills to convince the victim to download and install the spyware. Therefore, companies should pay great attention to protecting the information from these types of attacks.

In general, we can sum up that organizations should take a comprehensive approach to information security issues and take legal, organizational, physical, hardware and software measures to protect information, taking into account the degree

of their value and confidentiality, as well as taking into account threats relevant to their field of activity.

## REFERENCES

1. Cho D. X., Nam H. H. – A method of monitoring and detecting APT attacks based on unknown domains. – «IEEE Access». – 2019. – pp. 1132-1142.

2. Colakoglu T. The problematic of competitive intelligence: How to evaluate and develop competitive intelligence. – «Procedia - Social and Behavioral Sciences». – 2011. – pp. 615-1623.

3. Domanetska I., Khaddad A., Krasovska H., Yeremenko B. – Corporate system users' identification by the keyboard handwriting based on neural networks. – «International journal of innovative technology and exploring engineering». – 2019. – pp. 4156-4161.

4. Feng B., Li Q., Ji Y., Guo D., Meng X. Stopping the cyberattack in the early stage: assessing the security risks of social network users. – «Security and Communication Networks». – 2019. – pp. 1-14.

5. Thorleuchter D., Van den Poel D. Protecting research and technology from espionage. – «Expert Systems with Applications». – 2013. – pp. 3432–3440.